PATENT
Docket No. **VIV/0018.01**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gregor P. Freund	Examiner: Mede, Esteve
Serial No.: 10/710,781	Art Unit: 2137
Filed: August 2, 2004	APPEAL BRIEF
For: System and Methodology for Protecting New Computers by Applying a Preconfigured Security Update Policy	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

BRIEF ON BEHALF OF GREGOR FREUND

This is an appeal from the Final Rejection mailed November 09, 2007, in which currently-pending claims 1-70 stand finally rejected. Appellant filed a Notice of Appeal on February 13, 2008. This brief is submitted electronically in support of Appellant's appeal.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is assignee Check Point Software Technologies, Inc. located at 800 Bridge Parkway, Redwood City, CA 94065.

2. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellant, the Appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

The status of all claims in the proceeding is as follows:

Rejected: Claims 1-70

Allowed or Confirmed: None

Withdrawn: None

Objected to: None

Canceled: None

Identification of claims that are being appealed: Claims 1-70

An appendix setting forth the claims involved in the appeal is included as the last section of this brief.

4. STATUS OF AMENDMENTS

One Amendment has been filed in this case. Appellant filed an Amendment on August 6, 2007, in response to a non-final Office Action dated May 4, 2007. In the Amendment, the pending claims were amended in a manner which Appellant believes clearly distinguished the claimed invention over the art of record, for overcoming the art rejections. In response to the Examiner's Final Rejection dated November 9, 2007, Appellant filed a Notice of Appeal. Appellant has chosen to forgo filing an Amendment After Final which might further limit Appellant's claims, as it is believed that further amendments to the claims are not warranted in view of the art. Accordingly, no Amendments have been entered in this case after the date of the Final Rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Appellant asserts that the art rejections herein fail to teach or suggest all of the

claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 1**: a method for controlling connections to a computer upon its initial deployment (see, e.g., Appellant's Specification generally at Fig. 4 and paragraphs [0059-0062], and Fig. 5 and paragraphs [0063-0068]), the method comprises steps of: upon the initial deployment of the computer, applying a preconfigured security update policy that establishes a restricted zone of at least one preapproved host that the computer may connect to upon its initial deployment, so that the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also *Protecting Newly Deployed Computers* section and "restricted" zone description thereat, at paragraphs [0048-0050],, and overview to pre-access restricted zone at paragraphs [0051-0052]); receiving a request for a connection from the computer to a particular host and based on the preconfigured security update policy, determining whether the particular host is within the restricted zone of at least one preapproved host (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also Appellant's Specification at Fig. 5 and paragraph [0066], as well as the pre-access restricted zone description at paragraphs [0051-0052]); blocking the connection if the particular host is not within the restricted zone of at least one preapproved host (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also Appellant's Specification at Fig. 5 and paragraph [0067], and the pre-access restricted zone description at paragraphs [0051-0052]); and once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the Internet (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also Appellant's Specification at Fig. 5 and paragraphs [0067-0068], and the pre-access restricted zone description at paragraphs [0051-0052]).

Appellant asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 26**: a computer system that is preconfigured to control connections upon the initial deployment (see, e.g., Appellant's Specification generally at Fig. 3 and paragraphs [0053-0058], and operation description

at Fig. 4 and paragraphs [0059-0062], and Fig. 5 and paragraphs [0063-0068]) that comprises: a computer (see, e.g., computer 100 of Fig. 1) having a preconfigured security update policy that establishes a restricted zone of at least one preapproved host that the computer may connect to upon the initial deployment of the computer, so that the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also *Protecting Newly Deployed Computers* section and "restricted" zone description thereat, at paragraphs [0048-0050], and overview to pre-access restricted zone at paragraphs [0051-0052]; see also security policy description at paragraph [0057], and definition of security policy at paragraph [0029]); a connectivity module for processing user requests for the computer to connect to a particular host (see, e.g., Appellant's Specification description of general TCP/IP connectivity for computers, which is described at paragraph [0046] and at paragraphs [0030-0034]); and a security module for determining whether the particular host is within the restricted zone of at least one preapproved host based on the preconfigured security update policy, and for blocking any attempt to connect to a host that is not within the restricted zone of at least one preapproved host, until the computer is brought into compliance with the security update policy (see, e.g., Appellant's Specification at security system 330 (Fig. 3) and paragraphs [0053-0058]; see also description of system operation at Fig. 4 and paragraphs [0060-0062], Fig. 5 and paragraphs [0067-0068], and the pre-access restricted zone description at paragraphs [0051-0052]).

Appellant asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 49**: a method for enforcing pre-access connectivity restrictions on a new machine so as to enforce security updates (see, e.g., Appellant's Specification generally at Fig. 4 and paragraphs [0059-0062], and Fig. 5 and paragraphs [0063-0068]), the method comprises steps of: detecting attempts to connect the new machine to other devices (see, e.g., Appellant's Specification at Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also *Protecting Newly Deployed Computers* section and "restricted" zone description thereat, at paragraphs [0048-0050], and overview to pre-access restricted zone at paragraphs [0051-

0052]); determining, based on an initial security update policy that establishes a restricted zone of acceptable connections, which devices the new machine is permitted to connect to, so that the machine is not allowed to participate with general connectivity to the Internet until security-relevant updates have been applied to the machine (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also *Protecting Newly Deployed Computers* section and "restricted" zone description thereat, at paragraphs [0048-0050], and overview to pre-access restricted zone at paragraphs [0051-0052]; see also security policy description at paragraph [0057], and definition of security policy at paragraph [0029]); and blocking any connection that attempts to connect the new machine to a device outside the restricted zone of acceptable connections, so that the machine cannot participate with general connectivity to the Internet until the machine is brought into compliance with the security update policy (see, e.g., Appellant's Specification at Fig. 4 and paragraphs [0060-0062]; see also Appellant's Specification at Fig. 5 and paragraphs [0067-0068], and the pre-access restricted zone description at paragraphs [0051-0052]).

6. GROUNDS OF REJECTION TO BE REVIEWED

The grounds presented on appeal are:

(1st) Whether claims 1-4, 8-19,22-29,33-44,47-52,56-67 and 70 are unpatentable under 35 U.S.C. 102(b) as being anticipated by Freund (US 5,987,611);

(2nd) Whether claims 5-6, 30-31 and 53-54 are unpatentable under 35 U.S.C. 103(a) as being obvious over Freund (US 5,987,611) in view of Perkins et al. (US 2004/0187028 A1);

(3rd) Whether claims 7, 32, and 55 are unpatentable under 35 U.S.C. 103(a) as being obvious over Freund (US 5,987,611) in view of Aroya (US 2004/0177274 A1); and

(4th) Whether claims 20-21, 45-46 and 68-69 are unpatentable under 35 U.S.C. 103(a) as being obvious over Freund (US 5,987,611) in view of Marchosky (US 2004/0117215 A1).

7. ARGUMENT

A. First Ground: Claims 1-4, 8-19, 22-29, 33-44, 47-52, 56-67 and 70 rejected under Section 102

1. General

Under Section 102, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, the reference fails to teach each and every element set forth in Appellant's independent claims, as well as other claims, and therefore fails to establish anticipation of the claimed invention under Section 102.

2. Claims 1-4, 8-19, 22-29, 33-44, 47-52, 56-67 and 70

Claims 1-4, 8-19, 22-29, 33-44, 47-52, 56-67 and 70 stand rejected under 35 U.S.C. 102(b) as being anticipated by Freund (US 5,987,611). Here, the Examiner has likened Appellant's claimed invention to Appellant's own prior patent:

> Regarding claims 1, 26 and 49, Freund discloses a method for controlling connections to a compute upon its initial deployment of the computer, applying a preconfigured security policy that establishes a restricted zone of at least one pre-approved host that the computer may connect to upon its initial deployment, so that the computer is not allowed to participate with general connectivity to the internet until security relevant updates have been completed (col. 14, lines 14-23; col. 15, lines 26-33; col. 16, lines 1-3); receiving a request for a connection from the compute to a particular host (col. 15, lines 14-16); based on said pre-configured security policy, determining whether the particular host is within the restricted zone of at least one pre-approved host (col. 15, lines 26-34; col. 16, lines 1-3); blocking said connection if said particular host is not within the restricted zone of at least one pre-approved host (col. 19, lines 61-66; col. 4 lines 1-4); and once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the internet (col. 14, lines 14-23; col. 15, lines 26-33; col. 16, lines 1-3).
>
> (Final Rejection, at paragraph 4)

Appellant believes that the present invention is patentably distinct from Appellant's

previously-patented invention.

To be sure, the underlying endpoint security system (commercial product of ZoneAlarm®), which is the subject of the' 611 patent, is owned by the present assignee and is used as part of the preferred embodiment of the present invention. However, an important distinction exists. The original ZoneAlarm® Security Suite product (as well as all other security products, including Norton, McAfee, etc.) have no notion of a "pre-access" firewall and access rules that limit a machine at the system level to only accessing specific sites (i.e., sites that the manufacture is aware of at the time that the image is built). In this manner, each machine receiving that configuration (disk image) will be limited to only contacting a limited set of security-relevant sites (i.e., pre-access restricted zone). Importantly, all other attempted connections to the machine (i.e., from non-approved addresses) are refused during the pre- and peri-access stage. Only upon a given machine completing updating of security subsystems is the machine's security policy updated to allow other connections to occur. In particular, until the machine has updated relevant security components, the machine is not allowed to participate with general connectivity to the Internet, and the user is informed that is unsafe to do so until the security-relevant updates have been completed. Quite simply, prior art versions of security software simply gave machines general connectivity to the Internet and provided firewall and antivirus protection with versions (and definition files) that were effectively guaranteed to be out-of-date by the time the machines reached consumer hands.

In accordance with the present invention, a new zone is introduced: a "restricted" zone (or "pre-access restricted zone") specifically for a new machine. Since the new machine operates in a restricted zone upon the initial deployment, the machine initially cannot be remotely accessed by another computer (e.g., a computer which is connected via a LAN or WAN). This restriction specifically addresses hacker probes, such as the MS-Blast worm (where infection can occur by virtue of a machine simply having Internet connectivity).

In order to bring these distinctions to the forefront, Appellant's claims were substantially amended (in the Amendment filed on August 6, 2007) to emphasize that the present invention is directed to enforcing pre-access connectivity restrictions on a new machine and emphasize that a "security update policy" is applied during this restricted

access stage. For example, Appellant's independent claims were amended to recite that "the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed." Here, the machine is restricted to only allow certain applications resident on the machine to connect to specific security-relevant sites that are specified in the security update policy (i.e., pre-access restricted zone). All other connections (e.g., from non-approved applications or processes, and/or to non-approved destinations) are denied. In other words, the user is effectively forced to apply relevant security updates before the machine is given general connectivity to the Internet. Importantly during this time, the machine simply cannot be infected (e.g., by a hacker scanning for an open port) since -- by default -- all other connections are denied. It is respectfully submitted that prior art versions of security software (including Appellant's own prior version of ZoneAlarm®, which is the subject of the' 611 patent) simply did not function in that manner and thus do not provide an adequate basis of prior art to anticipate Appellant's claimed invention.

In response to Appellant's arguments, the Examiner states in the Final Rejection (at paragraph 9 .1):

> Applicant argues that the prior art does not teach a pre-access firewall and access rules that limit a machine at the system level to only accessing specific sites. Examiner disagrees, the prior art discloses that the client system only allows or/and disallows connection to website base on the name of the website or/and the website IP address (Col. 19, lines 44-67; col. 20, lines 44-49; col. 24, lines 4-5).

Here, the Examiner sets up a strawman argument by misstating Appellant's position and invention. For example, the Examiner states, "Applicant argues that the prior art does not teach a pre-access firewall and access rules that limit a machine at the system level to only accessing specific sites," but the actual claim language instead states (among other things):

> upon the initial deployment of the computer, **applying a preconfigured security update policy that establishes a restricted zone** of at least one preapproved host that the computer may connect to upon its initial deployment, **so that the computer is not allowed to participate**

with general connectivity to the Internet until security-relevant updates have been completed;

(Claim 1, first subparagraph; Emphasis added.)

Here, the first claim limitation does not merely specify an initial default configuration for the firewall, as suggested by the Examiner. Instead, the claim limitation is directed to enforcing pre-access connectivity restrictions on a new machine and emphasizes that a "security **update** policy" is applied during this restricted access stage. This is not just a firewall having some default set of sites that are approved for connection. Significantly, the restricted zone is enforced (to absolutely prevent all other connectivity of the computer) until such time as the security update policy has been complied with. This is computer-implemented logic that has the specific additional effect of obliging or forcing the user to update his or her new computer before the general Internet connectivity is allowed. Equally important, this prevents Internet-borne threats (e.g., malware, viruses, Trojans, worms, and the like) from getting a "jump" on the user -- that is, infecting the new machine before the user has had an adequate opportunity to update firewall and virus files (e.g., definition files and program updates, if any), which would have prevented such an infection.

Even if the Examiner reconfigured Appellant's popular ZoneAlarm® product, in the manner that the Examiner contends anticipates the present invention, the result of that would not work to reproduce the result of the present invention. The missing ingredient is that Appellant's own prior ZoneAlarm® commercial product did not include functionality to force the user -- in a fairly insistent if not paternalistic manner -- to upgrade virus and firewall files before general Internet connectivity is granted. Instead, upon a user receiving a new computer configured in the manner that the Examiner contends reproduces the present invention, the user may simply modify the default configuration, adding whatever websites (and opening whatever ports) he or she chooses. With the present invention, the user cannot do this. The update must be performed before general Internet connectivity is permitted.

Similarly, the Examiner at paragraph 9.2 in the Final Rejection cites network-centric or server-centric approaches as anticipating Appellant's invention. For example,

the Examiner cites the '611 patent to point out that a new client on the network is allowed Internet connectivity once it is certified by a supervisor computer on the network. Importantly, the Examiner is pointing to enforcement mechanisms extrinsic or outside the new computer to carry out this certification and enforcement. That approach may work fine for a user connecting a new computer to a corporate network or other protected network, where safeguards are put in place by IT personnel. The approach does not work, however, when the user connects a new computer to a network lacking such protection. For example, if the user first connects his or her new computer to the Internet while at home or while at a public WiFi spot (i.e., at unprotected networks), the approach fails as there is no supervisor computer in place to make sure that user carries out the necessary security-related updates prior to getting full Internet connectivity for the new computer. Thus, to prevent the problem posed by such unprotected networks, it was necessary to invent an intrinsic enforcement mechanism (i.e., Appellant's restricted zone functionality) that would effectively achieve the same "supervisor computer" functionality pointed to by the Examiner, but do so within the confines of a given new machine, all without having to rely on a supervisor computer or network-provided security to provide such features, as those may in fact not be present.

3. Conclusion

For the reasons stated, it is respectfully submitted that the claims set forth a patentable advance over the art, and that the rejection under Section 102 is improper. Accordingly, it is respectfully requested that the Examiner's rejection not be sustained.

B. Second Ground: Claims 5-6, 30-31 and 53-54 rejected under Section 103

1. General

Under Section 103(a), a patent may not be obtained if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. To establish a prima facie case of obviousness under this section, the Examiner must establish: (1) that there is some suggestion or motivation, either in the references themselves or in the knowledge

generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, (2) that there is a reasonable expectation of success, and (3) that the prior art reference (or references when combined) must teach or suggest all the claim limitations. (See e.g., MPEP 2142). The references cited by the Examiner fail to meet these conditions.

2. Claims 5-6, 30-31 and 53-54

Claims 5-6, 30-31 and 53-54 stand rejected under 35 U.S.C. 103(a) as being obvious over Freund (US 5,987,611) in view of Perkins et al. (US 2004/0187028 A1). Here, the Examiner repeats the rejection based on the Freund above, but adds Perkins for the contention that it teaches the claim limitation of "wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment." The claims are believed to be allowable for at least the reasons cited above pertain to the Section 102 rejection. Perkins itself includes no teaching overcoming this deficiency.

As stated above, Appellant's independent claims were amended to emphasize that a "security update policy" is applied during this restricted access stage, for limiting the computer's connectivity. This is computer-implemented logic intrinsic to the new computer (i.e., not requiring external supervisor computer or network-based security module) that has the specific additional effect of obliging or forcing the user to update his or her new computer before the general Internet connectivity is allowed. Importantly, the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed, even if the new computer is connected to a totally unprotected network. As none of the prior art systems (including Appellant's own' 611 patent) functioned in that manner, it is respectfully submitted that those systems do not provide an adequate basis of prior art to teach or suggest Appellant's claimed invention, or render Appellant's invention obvious in view of Perkins.

3. Conclusion

It is respectfully submitted that the claims set forth a patentable advance over the art, and that any rejection under Section 103 is improper. Accordingly, it is respectfully

requested that the Examiner's rejection not be sustained.

C. Third Ground: Claims 7, 32, and 55 rejected under Section 103

1. Claims 7, 32, and 55

Claims 7, 32, and 55 stand rejected under 35 U.S.C. 103(a) as being obvious over Freund (US 5,987,611) in view of Aroya (US 2004/0177274 A1). Here, the Examiner repeats the rejection based on the Freund above, but adds Aroya for the contention that it teaches the claim limitation pertaining to preventing the computer from being infected by a malicious program delivered through an open port. The claims are believed to be allowable for at least the reasons cited above pertain to the Section 102 rejection. Aroya itself includes no teaching overcoming this deficiency. Simply put, the prior art references when combined do not teach or suggest all the claim limitations, and thus do not form a competent rejection under Section 103. Accordingly, it is respectfully requested that the rejection not be sustained.

D. Fourth Ground: Claims 20-21, 45-46 and 68-69 rejected under Section 103

1. Claims 20-21, 45-46 and 68-69

Claims 20-21, 45-46 and 68-69 are unpatentable under 35 U.S.C. 103(a) as being obvious over Freund (US 5,987,611) in view of Marchosky (US 2004/0117215 A1). Here, the Examiner repeats the rejection based on the Freund above, but adds Marchosky for the contention that it teaches the claim limitation pertaining to providing a warning to user and displaying a disclaimer to user. The claims are believed to be allowable for at least the reasons cited above pertain to the Section 102 rejection. Marchosky itself includes no teaching overcoming this deficiency. Again, the Examiner has formulated a combination of prior art references that do not teach or suggest all the claim limitations. As these combined references do not form a competent rejection under Section 103, it is respectfully requested that the rejection not be sustained.

C. Conclusion

The present invention greatly improves the ease and efficiency of the task

deploying a new computer anywhere (including on unprotected networks) in such a manner that makes it impossible for the computer to get infected with malware before the user has had an opportunity to update security related files (e.g., firewall and virus definition files). It is respectfully submitted that the present invention, as set forth in the pending claims, sets forth a patentable advance over the art.

In view of the above, it is respectfully submitted that the Examiner's rejections under 35 U.S.C. Section 102 and 103 should not be sustained. If needed, Appellant's undersigned attorney can be reached at 408 884 1507. For the fee due for this Appeal Brief, please refer to the attached Fee Transmittal Sheet. This Brief is submitted electronically.

Respectfully submitted,

Date: May 13, 2008

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX

8. CLAIMS APPENDIX

1. A method for controlling connections to a computer upon its initial deployment, the method comprising:

upon the initial deployment of the computer, applying a preconfigured security update policy that establishes a restricted zone of at least one preapproved host that the computer may connect to upon its initial deployment, so that the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed;

receiving a request for a connection from the computer to a particular host;

based on said preconfigured security update policy, determining whether the particular host is within the restricted zone of at least one preapproved host;

blocking said connection if said particular host is not within the restricted zone of at least one preapproved host; and

once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the Internet.

2. The method of claim 1, further comprising:

prior to the initial deployment of the computer, imaging a hard disk of the computer with said preconfigured security update policy.

3. The method of claim 1, wherein the computer comprises a portable computer and the initial deployment includes establishing Internet connectivity.

4. The method of claim 1, wherein the restricted zone comprises a pre-access restricted zone specifically for a new machine.

5. The method of claim 1, wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment.

6. The method of claim 1, wherein said preconfigured security update policy operates to prevent the computer from being remotely probed for vulnerabilities by other computers.

7. The method of claim 1, wherein said preconfigured security update policy operates to prevent the computer from being infected by a malicious program delivered through an open port.

8. The method of claim 1, wherein said blocking step includes:

instructing a firewall, which is responsive to said preconfigured security update policy, to block connections to any host that is not within the restricted zone of at least one preapproved host.

9. The method of claim 1, wherein the at least one preapproved host comprises specific security-relevant sites.

10. The method of claim 9, wherein specific security-relevant sites include antivirus Web sites.

11. The method of claim 9, wherein specific security-relevant sites include firewall Web sites.

12. The method of claim 9, wherein specific security-relevant sites include end point security Web sites.

13. The method of claim 1, wherein other attempted connections to the computer are refused.

14. The method of claim 1, further comprising:

upon the computer completing updating of security subsystems, removing the restricted zone so that the computer may connect to other machines.

15. The method of claim 14, wherein the restricted zone is removed by replacing the preconfigured security update policy with an updated security update policy.

16. The method of claim 1, wherein the preconfigured security update policy is preinstalled on the computer prior to user purchase.

17. The method of claim 1, wherein the computer includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk image includes the preconfigured security update policy.

18. The method of claim 1, wherein the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been performed.

19. The method of claim 18, further comprising:

providing an option that allows a user to override the preconfigured security update policy.

20. The method of claim 19, further comprising:

providing a warning to any user that overrides the preconfigured security update policy.

21. The method of claim 19, further comprising:

displaying a disclaimer to any user that overrides the preconfigured security update policy that indicates that the user assumes responsibility.

22. The method of claim 9, wherein specific security-relevant sites include operating system-related Web sites.

23. The method of claim 1, further comprising:

upon a first attempted connection of the computer, downloading an updated list of hosts that the computer may initially connect to.

24. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

25. A downloadable set of processor-executable instructions for performing the method of claim 1.

26. A computer system that is preconfigured to control connections upon the initial deployment, the system comprising:

a computer having a preconfigured security update policy that establishes a restricted zone of at least one preapproved host that the computer may connect to upon the initial deployment of the computer, so that the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed;

a connectivity module for processing user requests for the computer to connect to a particular host; and

a security module for determining whether the particular host is within the restricted zone of at least one preapproved host based on said preconfigured security update policy, and for blocking any attempt to connect to a host that is not within the restricted zone of at least one preapproved host, until the computer is brought into compliance with the security update policy.

27. The system of claim 26, further comprising:

a hard disk that receives a hard disk image having said preconfigured security update policy.

28. The system of claim 26, wherein the computer comprises a portable computer and the initial deployment includes establishing Internet connectivity.

29. The system of claim 26, wherein the restricted zone comprises a pre-access restricted zone specifically for a new machine.

30. The system of claim 26, wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment.

31. The system of claim 26, wherein said preconfigured security update policy operates to prevent the computer from being remotely probed for vulnerabilities by other computers.

32. The system of claim 26, wherein said preconfigured security update policy operates to prevent the computer from being infected by a malicious program delivered through an open port.

33. The system of claim 26, wherein the security module blocks attempts by instructing a firewall, which is responsive to said preconfigured security update policy, to block connections to any host that is not within the restricted zone of at least one preapproved host.

34. The system of claim 26, wherein the at least one preapproved host comprises specific security-relevant sites.

35. The system of claim 34, wherein specific security-relevant sites include antivirus Web sites.

36. The system of claim 34, wherein specific security-relevant sites include firewall Web sites.

37. The system of claim 34, wherein specific security-relevant sites include end point security Web sites.

38. The system of claim 26, wherein other attempted connections to the computer are refused.

39. The system of claim 26, further comprising:

a module for removing the restricted zone so that the computer may connect to other machines.

40. The system of claim 39, wherein the restricted zone is removed by replacing the preconfigured security update policy with an updated security update policy.

41. The system of claim 26, wherein the preconfigured security update policy is preinstalled on the computer prior to user purchase.

42. The system of claim 26, wherein the computer includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk image includes said preconfigured security update policy.

43. The system of claim 26, wherein the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been performed.

44. The system of claim 43, wherein the security module includes an option that allows a user to override the preconfigured security update policy.

45. The system of claim 44, wherein the security module displays a warning to any user that overrides the preconfigured security update policy.

46. The system of claim 44, wherein the security module displays a disclaimer to any user that overrides the preconfigured security update policy that indicates that the user assumes responsibility.

47. The system of claim 34, wherein specific security-relevant sites include operating system-related Web sites.

48. The system of claim 26, wherein the security module downloads an updated list of hosts that the computer may initially connect to.

49. A method for enforcing pre-access connectivity restrictions on a new machine so as to enforce security updates, the method comprising:

detecting attempts to connect the new machine to other devices;

determining, based on an initial security update policy that establishes a restricted zone of acceptable connections, which devices the new machine is permitted to connect to, so that the machine is not allowed to participate with general connectivity to the Internet until security-relevant updates have been applied to the machine; and

blocking any connection that attempts to connect the new machine to a device outside the restricted zone of acceptable connections, so that the machine cannot participate with general connectivity to the Internet until the machine is brought into compliance with the security update policy.

50. The method of claim 49, further comprising:

prior to the initial deployment of the new machine, imaging a hard disk of the new machine with said initial security update policy.

51. The method of claim 49, wherein the new machine comprises a portable computer and the initial deployment includes establishing Internet connectivity.

52. The method of claim 49, wherein said restricted zone comprises a pre-access restricted zone specifically for a new machine.

53. The method of claim 49, wherein said initial security update policy operates to prevent the new machine from being remotely accessed by another computer upon the

initial deployment.

54. The method of claim 49, wherein said initial security update policy operates to prevent the new machine from being remotely probed for vulnerabilities by other computers.

55. The method of claim 49, wherein said initial security update policy operates to prevent the new machine from being infected by a malicious program delivered through an open port.

56. The method of claim 49, wherein said blocking step includes:

instructing a firewall, which is responsive to said initial security update policy, to block connections to any host that is not within the restricted zone of at least one preapproved host.

57. The method of claim 56, wherein the at least one preapproved host comprises specific security-relevant sites.

58. The method of claim 57, wherein specific security-relevant sites include antivirus Web sites.

59. The method of claim 57, wherein specific security-relevant sites include firewall Web sites.

60. The method of claim 57, wherein specific security-relevant sites include end point security Web sites.

61. The method of claim 49, wherein other attempted connections to the new machine are refused.

62. The method of claim 49, further comprising:

upon the new machine completing updating of security subsystems, removing the restricted zone so that the new machine may connect to other machines.

63. The method of claim 62, wherein the restricted zone is removed by replacing the initial security update policy with an updated security update policy.

64. The method of claim 49, wherein the initial security update policy is preinstalled on the new machine prior to user purchase.

65. The method of claim 49, wherein the new machine includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk image includes said initial security update policy.

66. The method of claim 49, wherein the new machine is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed.

67. The method of claim 66, further comprising:

providing an option that allows a user to override the initial security update policy.

68. The method of claim 67, further comprising:

providing a warning to any user that overrides the initial security update policy.

69. The method of claim 67, further comprising:

displaying a disclaimer to any user that overrides the initial security update policy that indicates that the user assumes responsibility.

70. The method of claim 57, wherein specific security-relevant sites include operating system-related Web sites.

9. EVIDENCE APPENDIX

This Appeal Brief is not accompanied by an evidence submission under §§ 1.130, 1.131, or 1.132.

10. RELATED PROCEEDINGS APPENDIX

Pursuant to Appellant's statement under Section 2, this Appeal Brief is not accompanied by any copies of decisions.